SyncThru™ Web Admin Service Administrator Manual

2007 Samsung Electronics Co., Ltd. All rights reserved.

This administrator's guide is provided for information purposes only. All information included herein is subject to change without notice. Samsung Electronics is not responsible for any direct o r indirect damages, arising from or related to use of this administrator's guide.

- SyncThru(TM) is a trade mark of Samsung Electronics Co., Ltd.
- Samsung and the Samsung logo are trademarks of Samsung Electronics Co., Ltd.
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)
- This product uses OpenSLP library. (http://www.openslp.org/)
- This product uses Xerces library.
- This product uses Xalan library. (http://xalan.apache.org/)
- This product uses NetSNMP library. (http://net-snmp.sourceforge.net/)
- This product uses SQLite library. (http://www.sqlite.org/docs.html)
- This product uses Boost library. (http://www.boost.org/libs/libraries.htm)
- This product uses QT library. (http://doc.trolltech.com/)

All other brand or product names are trademarks of their respective companies or organizations.

CONTENTS

1 Introducing the SyncThru ™ Web Admin Service

Overview 1
Features 1
Benefits 2

2 Getting Started

3 Installing SyncThru ™ Web Admin Service

Installation Environment 5
Installing SyncThru ™ Web Admin Service 5
Viewing SyncThru ™ Web Admin Service 6
Stopping and Starting SyncThru ™ Web Admin Service 6
Uninstalling SyncThru ™ Web Admin Service 7
Upgrading SyncThru ™ Web Admin Service 7

4 Discovery

Starting Discovery 8
Scheduling Discovery 8
Discovery Strategy 9
Discovery Methods 9
Discovery Results 10
Device Group Management 10

5 Security

HTTPS 11
Authentication 11
SNMPv3 12

6 Email Settings

7 Troubleshooting

Forgotten password 14
Log-in error 15
Not accessible using a browser 16
Unable to find some network-connected devices 16
Device status appears incorrect 17
Authentication enabling doesn’t work 18
Firmware uploading and updating is too slow 19
The requested page was not found 20

8 Frequently Asked Questions

How do I get to the SyncThru ™ Web Admin Service after installing? 21
How do I discover devices? 21
Is there any way to speed up device discovery? 21
How do I push security configuration to printers? 22

How do I delete devices disconnected on the list? 23
What happens if I delete a device from the **Device list**? 24
I can see more than one entry with the same IP address in the **Device list**; what may be the reason? 24
How do I enable authentication? 24
What is the purpose of group management? 28
How do I manage jobs on the hard disk of each printer on SyncThru ™ Web Admin Service? 28
What is the SyncThru ™ Web Admin Service Plug-In and how does one use it? 30
Is it possible to add a list of multiple users? 30
How do I upgrade the firmware for devices? 30
What is the difference between **Clear devices in database** and **Clear Database**? 32
How do I contact the Samsung printer service for questions about SyncThru ™ Web Admin Service? 33
How do I contact a representative of administrators or send him email? 33
Is Window XP Service Pack 2 supported with SyncThru ™ Web Admin Service? 33

9 MIB References

Generic Support 34
Supported Printers 34

10 Acronyms and Abbreviations

1 Introducing the SyncThru ™ Web Admin Service

This chapter introduces you the SyncThru ™ Web Admin Service.

This chapter includes:

- **Overview**
- **Features**
- **Benefits**

Overview

SyncThru ™ Web Admin Service is a web-based management tool for configuring printers and other devices, checking device status, performing remote diagnostics, receiving alerts when possible problems occur, and changing settings without leaving your desk.

Features

Key functions:

- Web browser based fleet management tool
- Detecting the network devices manually or according to a schedule
- Generating the list of devices detected, with detailed information on each individual device
- Grouping the devices and managing the groups
- Loading firmware images to the SyncThru server and upgrading firmware for the device
- Setting the IP address for newly detected devices

Additional plug-in components:

- Device Cloning Plug-In
  To provide functionality for saving, storing and uploading device settings from one device to another device(s)
- Driver Management Plug-In
  To manage device drivers including the following functions:
  - Monitoring availability of new driver versions for Samsung network printers and multi-functional devices, downloading these new versions either automatically or manually, and storing them in the Driver Management Plug-In database
  - Installing printer drivers on remote computers
  - Configuring printer drivers on remote computers
  - Deleting printer drivers from remote computers
- File Storage Plug-In
  To manage files such as fonts, macros and forms stored on the Samsung devices

- Job Accounting Plug-In
  To provide Job Accounting functionality for print, scan, copy and fax jobs with permissions and limits.
- Local Device Discovery Plug-In
  To manage devices attached directly to remote computers using USB or LPT interfaces
- Report Generator Plug-In
  To report various information such as status, usage data, alert history or Job Accounting details.
- Device Location Plug-In
  To see the device information with a map
- SMS Plug-In
  To get the simple message service when no toner or low toner status is generated

Benefits

SyncThru ™ Web Admin Service provides easy and convenient printer management using a web browser. Centralized network printer management capability makes it easy for you to manage printers located on a large-scale network.

Economical:

- IT staff can improve job efficiency by decreasing manual device handling.
- Your company can save money by decreasing device error time.

Easy to install:

- You only have to install SyncThru ™ Web Admin Service once on a machine that is centrally connected on the network.
- You do not have to configure the web server. SyncThru ™ Web Admin Service sets up the web server automatically.
- You do not have to configure the database system. SyncThru ™ Web Admin Service sets up the SQLite database system automatically.
- You do not have to install any additional software on client machines.

Convenient:

- SyncThru ™ Web Admin Service provides intuitive UI and useful operation about device management.

Centralized Management:

- SyncThru ™ Web Admin Service provides powerful and various information about devices.
- You can handle and monitor devices on the network in a centralized way.

Enhanced features:

- You can add additional features easily by installing plug-ins.

2 Getting Started

Use this chapter when you get started with SyncThru TM Web Admin Service. Basic setup tasks are as follows:

- Install SyncThru TM Web Admin Service: See **3. Installing SyncThru TM Web Admin Service**.
- Search for devices on the network using Configure Discovery Methods: See **4. Discovery**.
- Set Security Options: See **5. Security**.
- Configure E-mail Settings: See **6. Email Settings**.

3 Installing SyncThru ™ Web Admin Service

This chapter includes:

- **Installation Environment**
- **Installing SyncThru TM Web Admin Service**
- **Viewing SyncThru TM Web Admin Service**
- **Stopping and Starting SyncThru TM Web Admin Service**
- **Uninstalling SyncThru TM Web Admin Service**
- **Upgrading SyncThru TM Web Admin Service**

Installation Environment

Items	Server System Requirements	Client System Requirements
Hardware	• 1 GHz or faster CPU • 256 MB RAM • 1.5 GB free disk space	• 1 GHz or faster CPU • 256 MB RAM
Operating Systems	• Windows 2000 • Windows XP • Windows 2003 Server • Windows Vista	• Any Operating System with required browser
Browsers	• Microsoft Internet Explorer 5.5 or a later version • Mozilla FireFox 1.0 or a later version	• Microsoft Internet Explorer 5.5 or a later version • Mozilla FireFox 1.0 or a later version

Note

- Operating systems such as Macintosh OS, Sun Solaris, Linux are not supported.
- For optimal viewing, screen resolution of the client system should be configured to 1024 by 768 pixels.

Installing SyncThru ™ Web Admin Service

To install SyncThru ™ Web Admin Service:

1. Go to the local or network location where you downloaded the Samsung SyncThru Web Admin Service installation file.
2. Start the **Setup.exe**.
3. Follow the instructions on the installation wizard.
   - The default destination path is **C**:**Program Files\Samsung Network Printer Utilities\SyncThru Web Admin Service**. You can change the path if desired.
   - The default port numbers for the web server: 8080 for HTTP and 8443 for HTTPS unless those are already in use. You can also change those values.
4. Click the **Finish** button.

Samsung SyncThru TM Web Admin Service runs on **Windows** service. It starts automatically after installation.

Viewing SyncThru TM Web Admin Service

To view SyncThru TM Web Admin Service in a supported web browser, type one of the following URLs:

- http://server_name.domain:port_number/
- http://ip_address:port_number/

Note

- server_name.domain is the hostname of the SyncThru TM Web Admin Service host machine.
- ip_address is the IP address of the machine where SyncThru TM Web Admin Service is installed.
- port_number is the port number that you entered during the installation.

For example, you can enter http://10.88.195.132:90 if you configure port number 90 for HTTP. If you use syncthru.solution.com with the host name for SyncThru TM Web Admin Service, you can enter http://syncthru.solution.com:90.

Stopping and Starting SyncThru TM Web Admin Service

SyncThru TM Web Admin Service is started automatically after installation. However, you might need to stop and start SyncThru manually sometimes.

To stop SyncThru TM Web Admin Service:

1. In the **Control Panel**, go to **Administrative Tools** > **Services**.
2. Select **SyncThru Web Admin Service** from the list.
3. Click **Stop** button.

To start SyncThru TM Web Admin Service:

1. In the **Control Panel**, go to **Administrative Tools** > **Services**.
2. Select **SyncThru Web Admin Service** from the list.
3. Click **Start** button.

Uninstalling SyncThru ™ Web Admin Service

> **Note**
> If you installed additional plug-ins, uninstalling of these plug-ins shall be required before SyncThru ™ Web Admin Service is removed.

You can use its own uninstaller at Windows **Start** menu. Or use the Windows **Add or Remove Programs** application to uninstall SyncThru ™ Web Admin Service.

1. In the **Control Panel**, double-click **Add or Remove Programs**.
2. Select **SyncThru Web Admin Service** and click **Change/Remove**.

> **Note**
> If you want to remove the SyncThru database file including device information, check the checkbox for **Remove SyncThru Web Admin Service information**. Otherwise, skip this option and just click the **Next** button.

3. Click the **OK** button to confirm the uninstallation.

Upgrading SyncThru ™ Web Admin Service

To upgrade SyncThru ™ Web Admin Service,

1. Run the new Samsung SyncThru ™ Web Admin Service installation file.
2. Follow the instructions on the installation wizard.
   - Select **Yes** for the question, Would you like to upgrade SyncThru Web Admin Service to the new version?
   - The port numbers for the web server: Ports that were configured in the previous version will be displayed. You can change to other ports if you want.
3. Click the **Finish** button.

4 Discovery

SyncThru ™ Web Admin Service lets you search your network for devices. You can then schedule and configure discoveries to suit your needs. Once devices are discovered, their information is stored on the server. To discover devices, you have to decide discovery method: **IP broadcast**, **SLP multicast**, and **IP Range**. After you discover devices, you can organize them to group referring to the Device **Group management**.

This chapter includes:

- **Starting Discovery**
- **Scheduling Discovery**
- **Discovery Strategy**
- **Discovery Methods**
- **Discovery Results**
- **Discovery Results**
- **Device Group Management**

Starting Discovery

How to start discovery:

1. Go to the **Devices** > **Discovery** > **Start discovery** page.
2. Configure the discovery settings.
3. Click the **Start discovery** button, then you can see the discovery status in the **Discovery results**.

By default, the **IP broadcast** discovery method is enabled. Because discovery time and accuracy depends on the network environments and which discovery methods you enable, choose the discovery methods according to the discovery strategy.

Scheduling Discovery

SyncThru ™ Web Admin Service provides a scheduling function for your efficiency. You can schedule discoveries to run automatically. You can schedule multiple, distinct discoveries by editing discovery schedules.

How to add a new scheduled discovery:

1. Go to the **Devices** > **Discovery** > **Schedule** page.
2. Click **Add schedule**.
3. Configure the **Start date** and **Time interval**.
4. Select discovery method you want and fill in the properties.
5. Click **Apply** button.

You can see the new schedule in the **Schedule List**. You can also edit or delete the specified schedule in the list.

Discovery Strategy

- To minimize the impact on other network traffic: Configure SyncThru ™ Web Admin Service to perform regularly scheduled discoveries during off-hours at intervals that are appropriate for your network environment.
- To search through a range of addresses for TCP/IP devices on local or remote networks: Use the **IP Range** discovery method for the local or remote network.
- To find new TCP/IP devices as they are added to the local network: Use the **IP broadcast** discovery method or add the devices manually in the **Device list**.
- To run a very quick discovery with some network traffic: Use the **IP broadcast** method or the **SLP multicast** method (you can use both of them).
- To discover devices on the local subnet: Use the **IP broadcast** method.
- To discover devices on more than one subnet: Use the **IP Range** method or the **SLP multicast** method.

Discovery Methods

IP broadcast

The **IP broadcast** discovery method sends a general SNMP request to all of the active devices on the local subnet and listens for responses from supported devices. This discovery is very fast, but it causes a high level of broadcast traffic because all of the devices respond at the same time. In addition, some responses could collide and never reach SyncThru ™ Web Admin Service.

IP broadcast discovery is required in the following cases:

- To search a small network with a few devices
- To search devices quickly
- To search a single subnet

SLP multicast

The **SLP multicast** discovery method sends a single SLP request over the specific multicast address, 239.255.255.253, defined by RFC 2608. Only the devices which support multicast IP address can respond to this request. This discovery is similar to the **IP broadcast** discovery except that it looks for only the specific devices. It means that it does not generate as much network traffic and is less likely to lose device responses.

SLP multicast discovery is required in the following cases:

- Search devices that support multicast broadcasts.

- Search devices on a relatively small network.

Note

Because the values of **Multicast address** and **Scope** for Samsung device are already embedded in this system, so you don't need to put it in manually. Port number 427 is always used for **SLP multicast** discovery. Make sure that SLP protocol is enabled on device. Otherwise, you need to contact your network administrator.

IP Range

The **IP Range** discovery method searches for the devices within a range of IP addresses. SyncThru ™ Web Admin Service can find devices on local or remote subnets. However it can be slow on large networks because an **IP Range** discovery checks each IP address including unused ones to see if a device is there. In other words, it can cause directed traffic on large networks.

IP Range discovery is required in the following cases:

- To discover devices on local and remote subnets
- To run a discovery for specific **IP Range**s with different schedules
- To limit the scope of discovery on the network

Note

Your network monitoring system might consider the discovery as being an attack to your network. Contact and inform your network administrator when running this discovery.

Discovery Results

You can see the list of discoveries completed as well as the discoveries in progress in the **Discovery results**. Four kinds of data display in the list: **State**, **Start time**, **End time** and **Found devices** with the number of **New devices**. Also, the following additional operations are provided.

- **Show found devices**: view the list of discovered devices
- **Cancel discovery**: cancel discovery in progress
- **Clear completed**: remove completed discoveries from the list

Device Group Management

You can organize devices into groups according to the location, department, or the other information for your site. After your discovery is completed, you can begin creating custom groups and assigning devices to them. You can manage groups in the **Devices** > **Group management**.

5 Security

SyncThru ™ Web Admin Service provides the following features for its network security:

- **HTTPS**
- **Authentication**
- **SNMPv3**

HTTPS

By default, SyncThru ™ Web Admin Service uses HTTP.

- If you want to change the HTTP port number, go to the **Settings** > **Web server configuration**. You can change the port number.
- If you want to use a secure connection, you can use HTTPS by enabling the SSL. Certificate settings are required before SSL enablement. All communications between SyncThru ™ Web Admin Service and a Web browser are sent encrypted using HTTPS.

Note

Make sure you enter https://ip_address:https_port_number in the web browser address bar when SSL is enabled. If you type http://ip_address:https_port_number or https://ip_address in the web browser address bar, the page will not load.

How to configure certificate settings:

1. Go to the **Settings** > **Web server configuration**.
2. You can click the **Certificate configuration** button. There are three options for certificate settings:
    - **Create self-signed certificate**: to create a certificate using SyncThru ™ Web Admin Service-provided functionality.
    - **Prepare certificate request**: to request the certificate from the external certificate authority.
    - **Upload existing certificate**: to upload the certificate already issued by the external or internal certificate authority.

Note

If there is no certificate installed, the **Certificate** area does not contain any information and the **Certificate status** area is not available.

Authentication

With a certificate installed, you can enable SSL to access SyncThru ™ Web Admin Service using HTTPS protocol. Then you can enable authentication to maintain SyncThru ™ Web Admin Service access rights. If no certificate is configured, **Enable authentication** button is unavailable.

By default, there is only the user of **admin** in the authentication list. Its password is also **admin** by default. You can change user settings in the **Settings** > **Authentication** page.

Note

Once authentication is enabled, the session will continue to be connected for 180 seconds. After 180 seconds, the user must log in again.

SNMPv3

This is related to the device security. You can configure the security settings for the devices which support SNMPv3 security (RFC2571). These devices will not report any status information until you set up the security configuration. The SNMPv3 protocol encrypts the information being sent between SyncThru ™ Web Admin Service and a device.

How to enable SNMPv3 feature:

1. Go to the **Device list**.
2. Select a device you want to set up the SNMPv3 security configuration.
3. Click the **Security configuration** button.
4. Fill in the following fields:

Menu	Description
Security level	Decide the security level which can be enabled for the device. • No authentication: no security checks are performed on devices. • Authentication: user authentication is enabled, but SNMP communications are not encrypted. • Authentication and encryption: user authentication is enabled and SNMP communications are encrypted.
User name	Type the user identifier.
Authentication password	Type the password which is used for user authentication if authentication is enabled.
Privacy password	Type the password used for encryption if encryption is enabled.
Authentication method	Select the method for security hash generation. • MD5: Message Digest algorithm 5 • SHA: Security Hash Algorithm
Context name	Type a contact name for collecting management information accessible by an SNMP entity.
Context ID	Type an identifier of an SNMP entity that may recognize an instance of a context with a particular context name.

6 Email Settings

You need to configure this feature for using SyncThru ™ Web Admin Service efficiently.

SMTP server settings are required for sending reports automatically.

How to set up the email service:

1. Go to the **Settings** > **SMTP server configuration**.
2. Fill in the following fields:

Menu	Description
SMTP server and port	Type the default port number is 25.
SMTP requires authentication	Check this box if authentication is required to access the server.
SMTP server login	Fill here if SMTP Requires Authentication is enabled.
SMTP server password	Fill here if SMTP Requires Authentication is enabled.
SMTP connection time-out	Type the time during which the system will try to connect to the SMTP server.
From address	Type the e-mail address which will be provided as the sender's address.

3. To verify whether the SMTP server configuration you filled is correct, fill the **Test destination address** textbox in **Test send** field.
4. Press the **Send** button.

7 Troubleshooting

This chapter gives helpful information on what to do if you encounter a problem.

This chapter includes:

- **Forgotten password**
- **Log-in error**
- **Not accessible using a browser**
- **Unable to find some network-connected devices**
- **Device status appears incorrect**
- **Authentication enabling doesn't work**
- **Firmware uploading and updating is too slow**
- **The requested page was not found**

Forgotten password

When you open SyncThru ™ Web Admin Service with the supported web browser, SyncThru ™ Web Admin Service requires a user name and its password, if authentication is enabled. If you have forgotten your password, you cannot log in and use SyncThru ™ Web Admin Service.

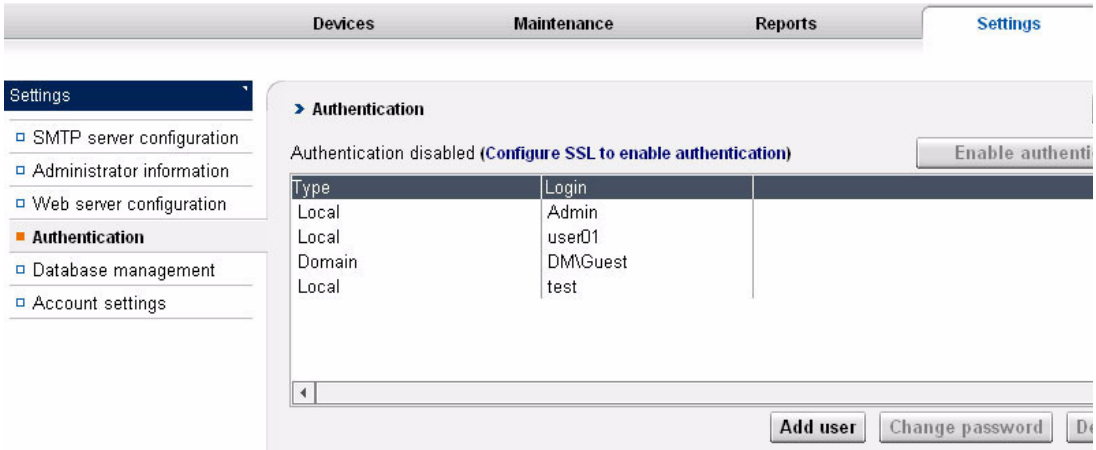
[User action]

Ask your administrator to reset your password.

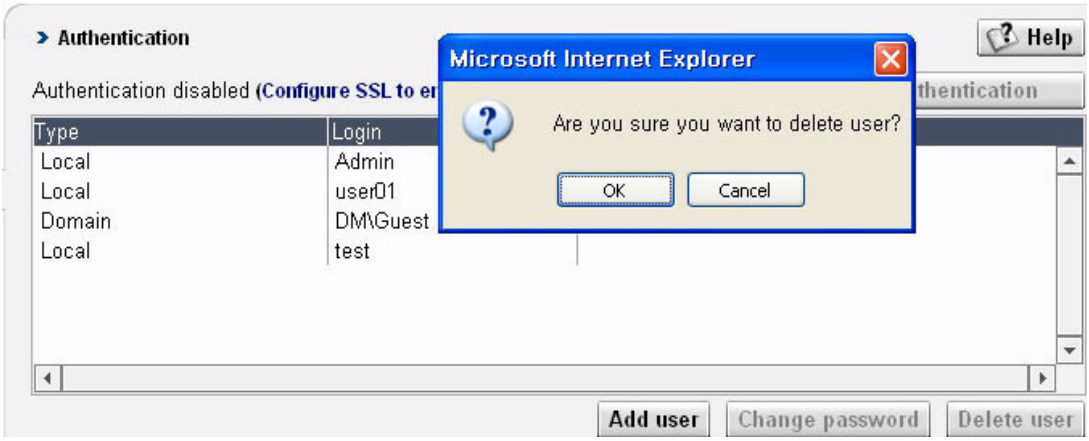
[Administrator action]

You should know your old password if you want to change your password. If a user has forgotten his password, you need to remove his user information and create new user information with the following steps:

1. Go to **Settings** > **Authentication**.
2. Select the appropriate user account.

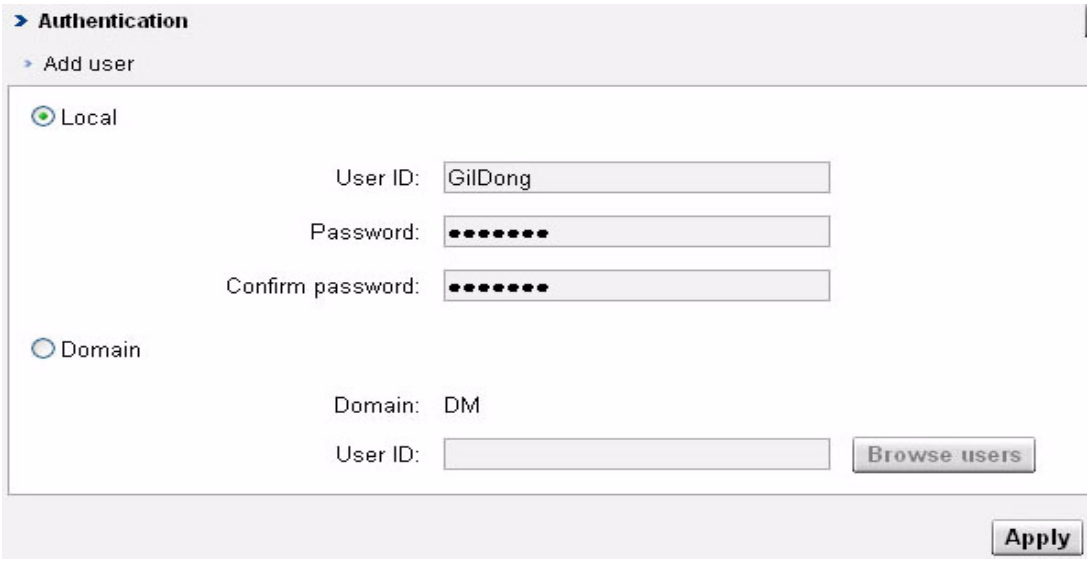


3. Click the **Delete user** button. Then you can remove the specified user.



4. After that, you need to create a new user account using the **Add user** button.

5. Set up the same as before.



Log-in error

When you open SyncThru ™ Web Admin Service with the supported web browser, a login user id and password will be required if authentication is enabled. You cannot log in with your own id and password.

[User actions]

- Verify your id and password, and ask your administrator whether your user id is in the SyncThru ™ Web Admin Service authentication list or not. If there is no id information for you, you need to ask your administrator to create your id.
- If there is wrong account information for you, ask your administrator to reset your user account.

[Administrator actions]

You can use the id of **admin** as a default user if you have not changed its information.

- If there is no such user in the authentication list, you need to create a new user id.
- If there is an appropriate user id in the authentication list, but a login error still happens, it means that the user information is incorrect. This is the same situation as **Forgotten password**. You need to remove the existing user account and add a new user.

Not accessible using a browser

When you open SyncThru ™ Web Admin Service from your browser, you cannot access it.

[User actions]

- Make sure of the URL and port number you type in the web browser.
- Check if your browser is supported by SyncThru ™ Web Admin Service.
- Ask your administrator.

[Administrator actions]

- Check if the SyncThru ™ Web Admin Service is running. If the service is not running, you need to restart the service. If the service is running, restart the system.
- Check if you can access SyncThru ™ Web Admin Service from your host machine, where SyncThru ™ Web Admin Service is installed. If you can access SyncThru ™ Web Admin Service from the host machine, but cannot access it from any remote machine, you may have a network issue that is preventing communication between the browser and the SyncThru ™ Web Admin Service host machine.
    - Ask your network administrator. You need to check your network policy, especially security issues.
    - Check the security settings, such as the firewall of the remote machine. If the port number of SyncThru ™ Web Admin Service is using is blocked with your network manager or firewall, you may have this problem.

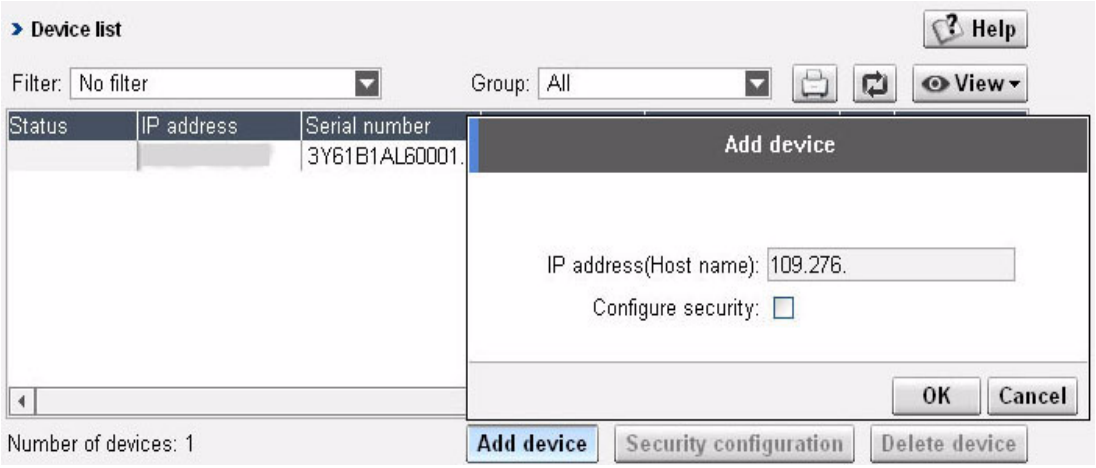
Unable to find some network-connected devices

SyncThru ™ Web Admin Service cannot discover some printers or MFPs on the network.

[Administrator actions]

- Make sure that the specified devices are turned on.
- The devices might have a network communication problem. Check the network configuration of the specified devices, such as protocol status.

- If you know the IP address of the devices that you want to find, you can add the devices using the **Add device** button, which is located in the **Devices** > **Device list** page.



- If your discovery has done with the **IP broadcast** method,
  - Run the discovery when there is less network traffic. If your network is busy, SyncThru ™ Web Admin Service might not discover some devices.
  - Try another discovery: **IP Range** method. If some devices are not on the same subnet, **IP broadcast** discovery might not find them.
- If your discovery has done with the **SLP multicast** method,
  - Make sure that the devices support multicast broadcasts. If the devices do not, try another discovery method.
  - Check whether the router is multicast-enabled or not. If the router is not enabled, the multicast packet does not go out of the router. You need to ask the network administrator to enable the multicast on the router.
  - If you want to find the devices on the remote subnets, you can change the multicast radius in the **Devices > Discovery > Start discovery**. The default radius value is 1 which is intended to search devices in one subnet boundary. There may be network issues according to your site policy of network environments.
- If your discovery has done with the **IP Range** method,
  - Check if the **IP Range** for the discovery reflects the network that is being scanned. Your network monitoring system might consider the discovery as being an attack to your network. If so, contact and inform your network administrator when running this discovery.
  - If SyncThru ™ Web Admin Service still cannot find the devices, the devices might have a network communication problem. Check the network configuration of the specified devices, such as protocol status.

Device status appears incorrect

You recognize that the device status appears incorrect.

[User & Administrator Actions]

If your network is busy or has a high level of network traffic, SyncThru ™ Web Admin Service might miss some packets.

- Make sure that the device is turned on.
- Refresh the device list by clicking the refresh button( )
- If this still happens, ask your network administrator about your network communication status.

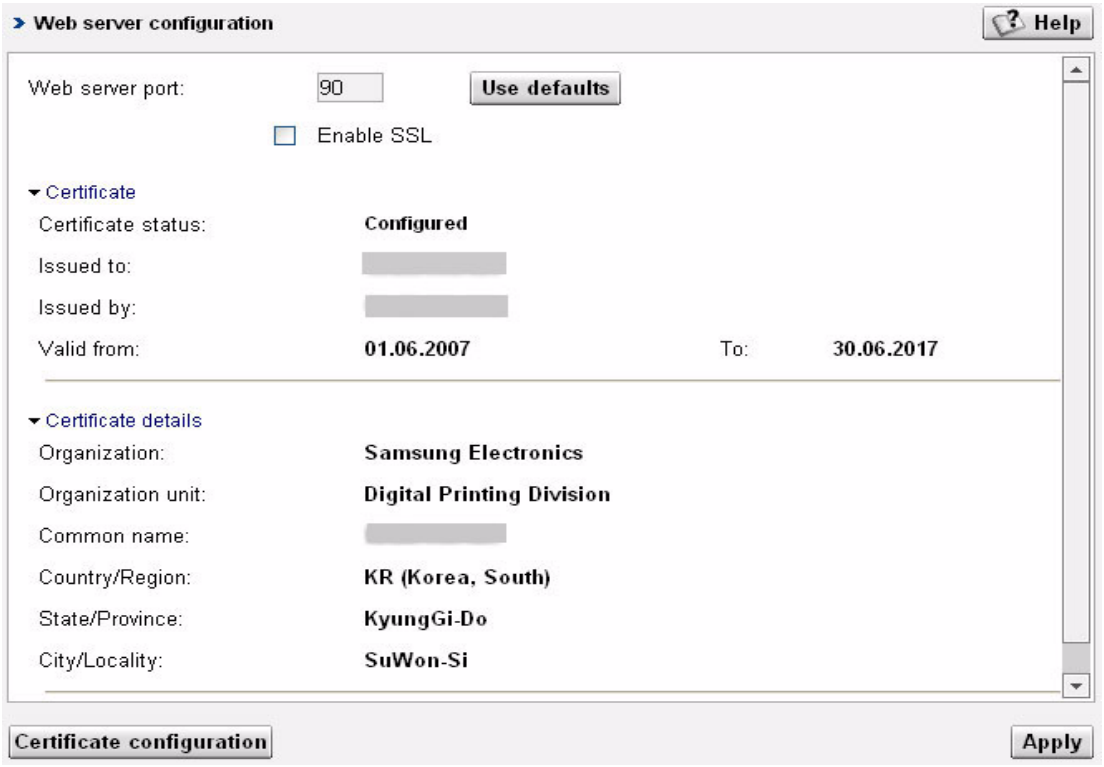
Authentication enabling doesn't work

You cannot enable the Authentication feature in SyncThru ™ Web Admin Service.

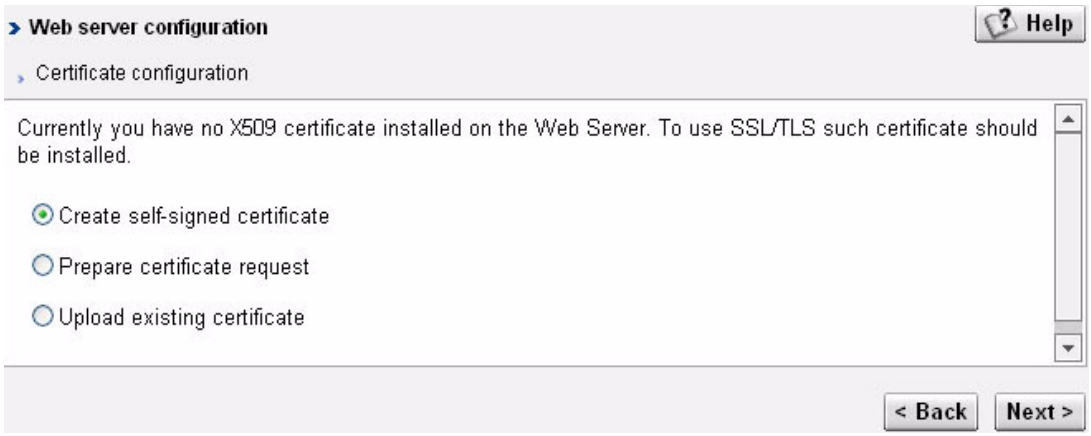
[Administrator Actions]

With a certificate installed, you can enable the SSL to access SyncThru ™ Web Admin Service using HTTPS protocol. Then you can enable authentication to maintain the access rights. If no certificate is configured, Authentication enablement is unavailable.

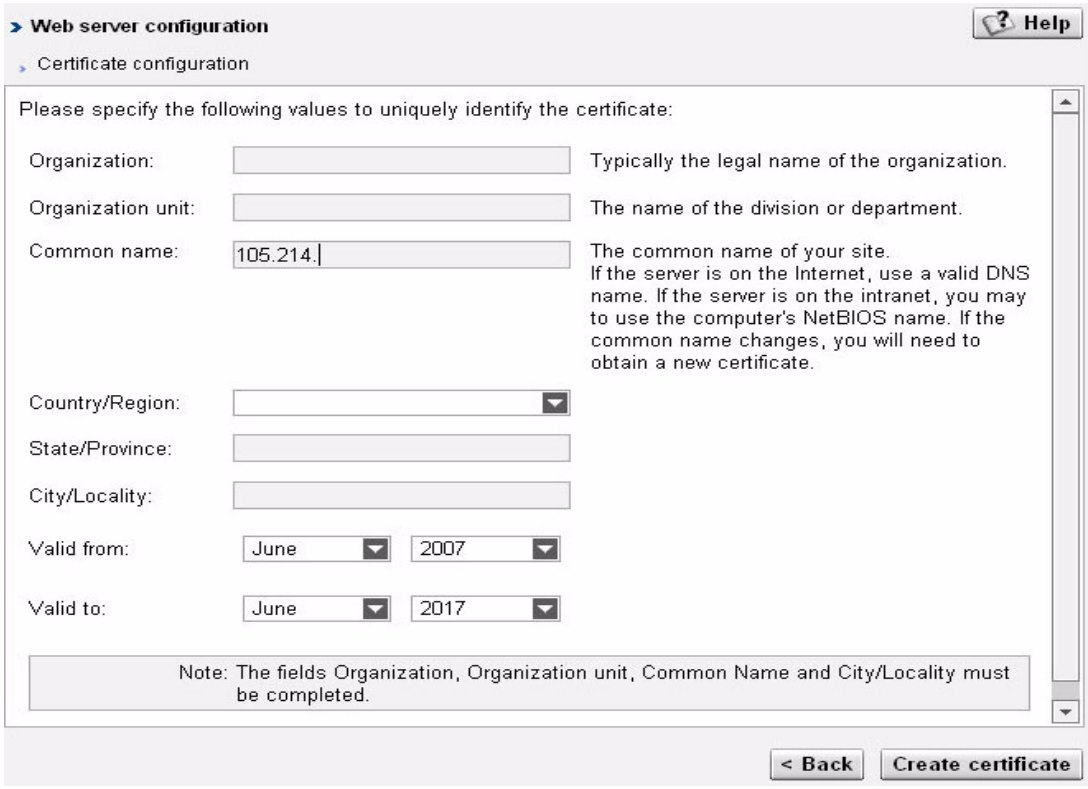
1. Make sure SSL is enabled.
2. Go to the **Settings > Web server configuration** page.
3. Click the **Certificate details** field**.** Then you can see the certificate details if you have installed a certificate. Otherwise, you need to install a new certificate using the **Certificate configuration** button.



4. Select the **Create self-signed certificate** in the **Web server configuration** page. Then click the **Next** button.


Web server configuration
Help
Certificate configuration
Currently you have no X509 certificate installed on the Web Server. To use SSL/TLS such certificate should be installed.
Create self-signed certificate
Prepare certificate request
Upload existing certificate
< Back
Next >

5. Enter the certificate information and click **Create certificate** button.


Web server configuration
Help
Certificate configuration
Please specify the following values to uniquely identify the certificate:
Organization:
Typically the legal name of the organization.
Organization unit:
The name of the division or department.
Common name:
105.214.
The common name of your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may to use the computer's NetBIOS name. If the common name changes, you will need to obtain a new certificate.
Country/Region:
State/Province:
City/Locality:
Valid from:
June
2007
Valid to:
June
2017
Note: The fields Organization, Organization unit, Common Name and City/Locality must be completed.
< Back
Create certificate

6. Check **Enable SSL** in **Settings > Web server configuration** page.

Firmware uploading and updating is too slow

When you upload firmware files or update device firmware, you have some speed problems.

[Administrator Actions]

In this case, there might be a network communication problem in your site. Ask your network administrator first. Another possibility may be the file size issue. It can take much longer time according to the file size.

The requested page was not found

When you access SyncThru ™ Web Admin Service and click any menu, you may encounter the error page displaying the message the requested page was not found. There might be unexpected errors or conflicts in the system.

[Administrator Actions]

- Make sure that the SyncThru ™ Web Admin Service is running. You need to restart SyncThru ™ Web Admin Service.
- Restart your SyncThru ™ Web Admin Service host machine.

8 Frequently Asked Questions

This chapter gives the answer of frequently asked questions.

This chapter includes:

- **How do I get to the SyncThru TM Web Admin Service after installing?**
- **How do I discover devices?**
- **Is there any way to speed up device discovery?**
- **How do I push security configuration to printers?**
- **How do I delete devices disconnected on the list?**
- **What happens if I delete a device from the Device list?**
- **I can see more than one entry with the same IP address in the Device list; what may be the reason?**
- **How do I enable authentication?**
- **What is the purpose of group management?**
- **How do I manage jobs on the hard disk of each printer on SyncThru TM Web Admin Service?**
- **What is the SyncThru TM Web Admin Service Plug-In and how does one use it?**
- **Is it possible to add a list of multiple users?**
- **How do I upgrade the firmware for devices?**
- **What is the difference between Clear devices in database and Clear Database?**
- **How do I contact the Samsung printer service for questions about SyncThru TM Web Admin Service?**
- **How do I contact a representative of administrators or send him email?**
- **Is Window XP Service Pack 2 supported with SyncThru TM Web Admin Service?**

How do I get to the SyncThru TM Web Admin Service after installing?

Go to the **Viewing SyncThru TM Web Admin Service** on page 6.

How do I discover devices?

SyncThru TM Web Admin Service provides 3 kind of discovery method: **IP broadcast**, **SLP multicast**, and **IP Range**. Go to the **Starting Discovery** on page 8.

Is there any way to speed up device discovery?

The current SyncThru TM Web Admin Service supports three discovery methods: **IP broadcast**, **SLP multicast**, and **IP Range**. Basically, **IP broadcast** and **SLP multicast** can discover with high speed while **IP Range** works slowly. If you have a speed problem with discovery, check the discovery strategy which recommended in **4. Discovery**. In the case of the **IP Range** method, refer to the following instructions:

- The **IP Range** discovery method checks every IP address. If the range includes many unused IP addresses, SyncThru TM Web Admin Service will check those addresses, which causes the speed problem. If you can ask your network administrator about the IP addressing schemes and network environments, or you already know them, this discovery can be faster.

- You can configure the specific range of IP addresses according to your network environments.
- If you want to use multiple, distinct **IP Range** settings, you can schedule your own discoveries. Go to the **Devices** > **Discovery** > **Schedule**. You can add specific schedules with **Add schedule**. For example, you can add a discovery schedule for searching a specific range of IP addresses in the afternoon.

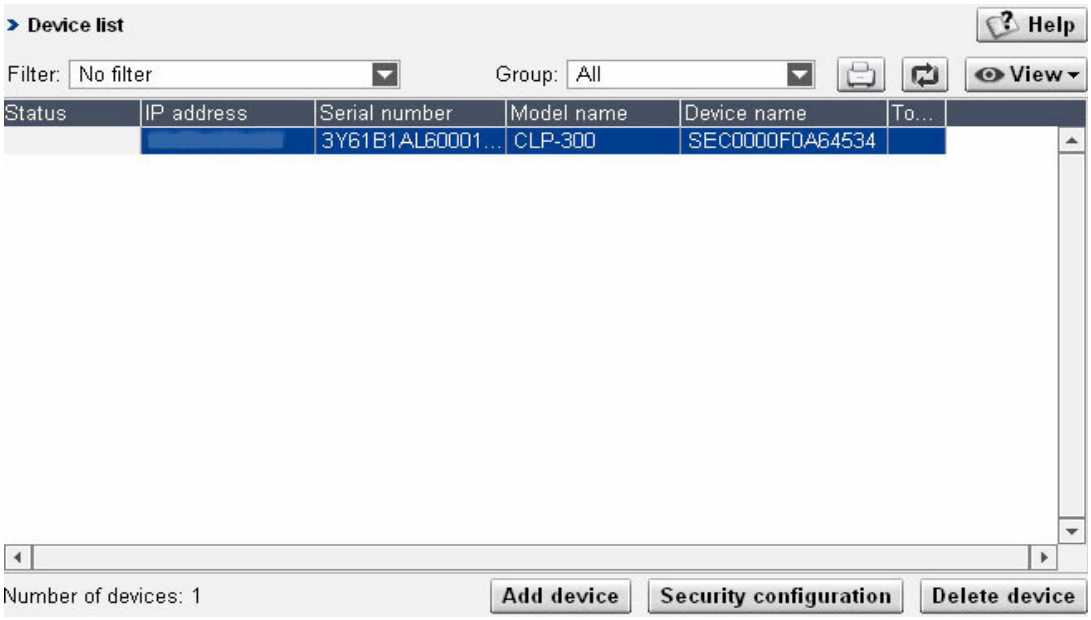
Note

SyncThru ™ Web Admin Service recommends that you run discoveries during off-hours if possible. Of course, all the devices must be turned on in this case.

How do I push security configuration to printers?

The security configuration for the printers can be enabled in SyncThru ™ Web Admin Service once discovery is finished.

1. Go to the **Devices** > **Device list** page and select appropriate device.
2. Click the **Security configuration** button.

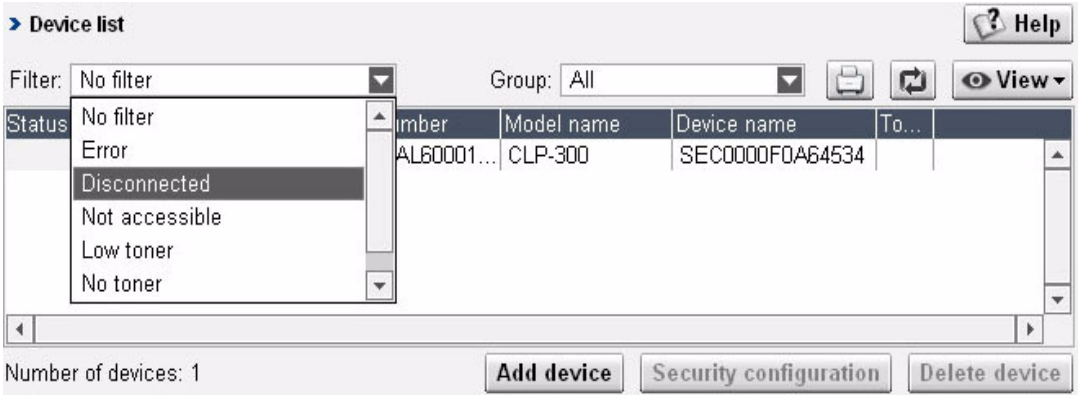


3. Configure secure settings and click the **Apply** button.

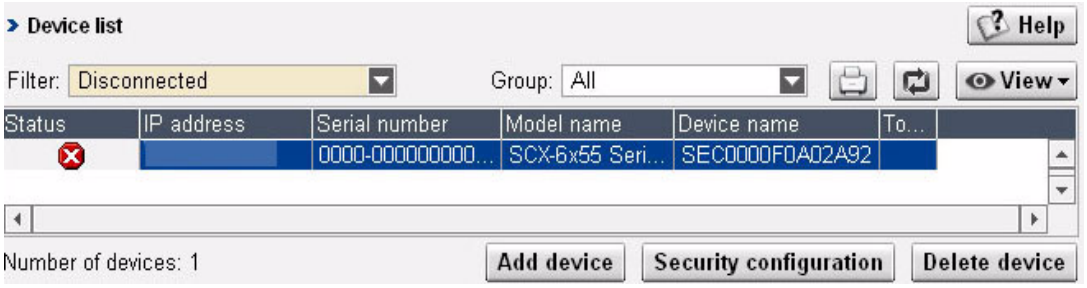
How do I delete devices disconnected on the list?

You can delete the disconnected devices using the filtering option.

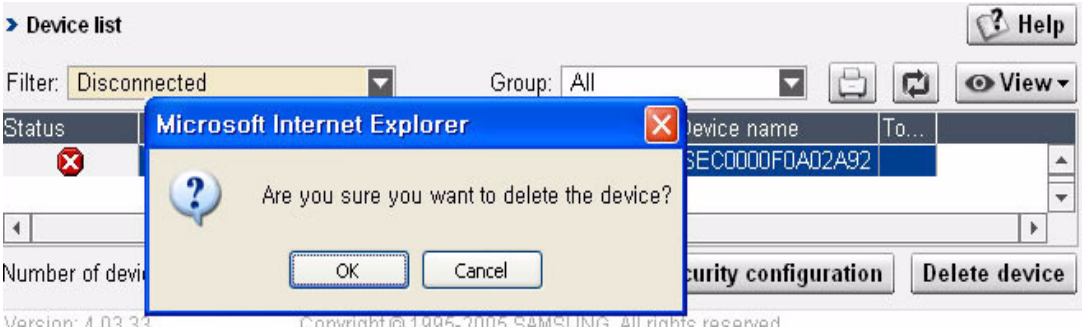
1. Go to the **Devices** > **Device list**.
2. You can see the drop-down list of the **Filter**. Select **Disconnected** in the list.



3. Then, you can see only disconnected devices in the **Device list**.



4. Now you can delete the devices using the **Delete device** button.



What happens if I delete a device from the Device list?

If you delete a device from the device list, SyncThru ™ Web Admin Service eliminates all information of the specified device. The SyncThru Database will not contain the device-related data any more.

I can see more than one entry with the same IP address in the Device list; what may be the reason?

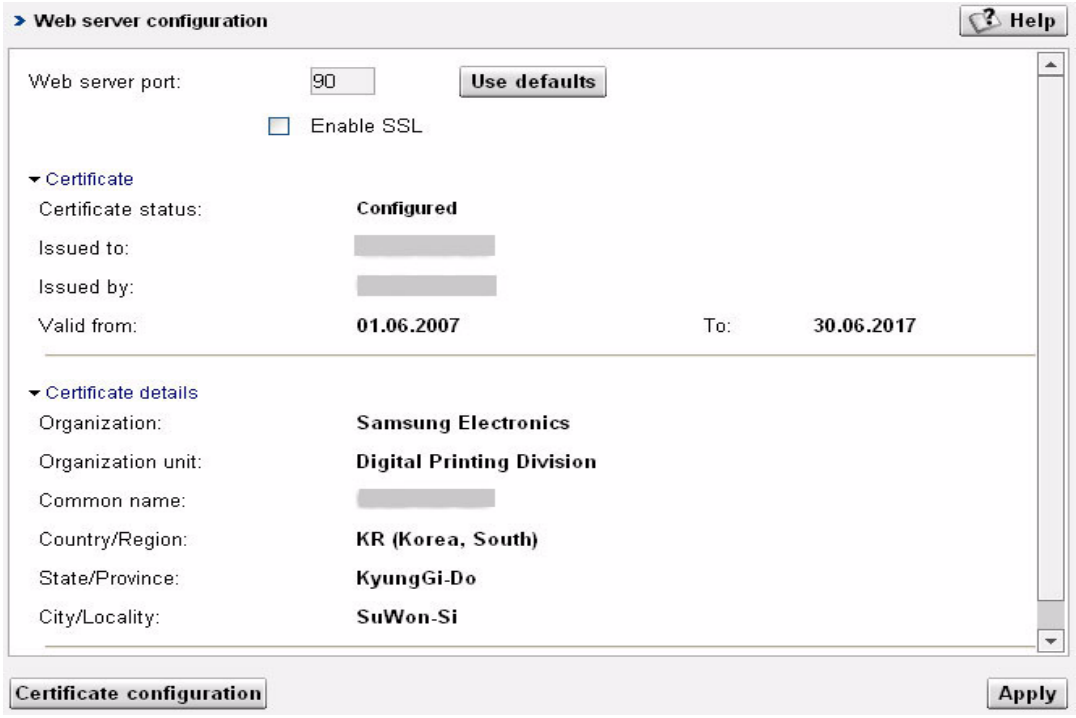
SyncThru ™ Web Admin Service uses the serial number and hardware address of the device as a unique key, so if your network environment uses dynamic IP addresses, the device list can contain more than one entry with the same IP address. To avoid this, delete devices that have the same IP, then restart discovery.

How do I enable authentication?

To enable authentication, certificate installation and SSL enablement are required. With a certificate installed, you can enable SSL to access SyncThru ™ Web Admin Service using HTTPS protocol. Then you can enable authentication to maintain the access rights.

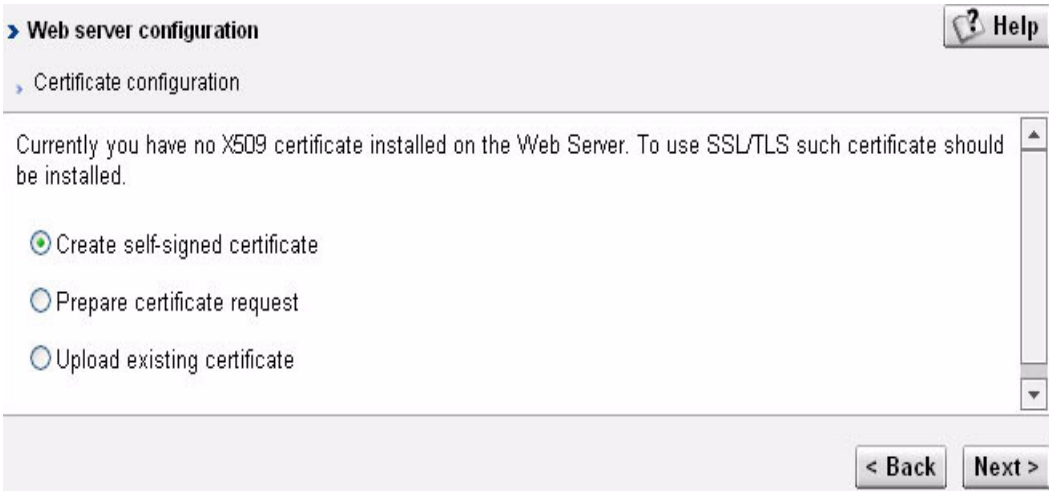
How to install a certificate:

1. Go to the **Settings** > **Web server configuration** page.



2. Click the **Certificate configuration** button.

   - **Create self-signed certificate**: to create a certificate using SyncThru ™ Web Admin Service-provided functionality.
   - **Prepare certificate request**: to request the certificate from the external certificate authority.
   - **Upload existing certificate**: to upload the certificate already issued by the external or internal certificate authority.

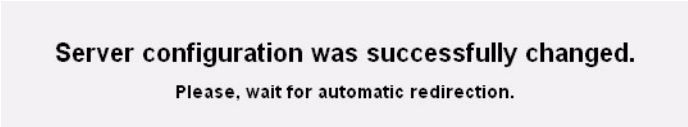

Web server configuration
Help
Certificate configuration
Currently you have no X509 certificate installed on the Web Server. To use SSL/TLS such certificate should be installed.
Create self-signed certificate
Prepare certificate request
Upload existing certificate
< Back
Next >

How to enable SSL:

1. Go to the **Settings** > **Web server configuration**.

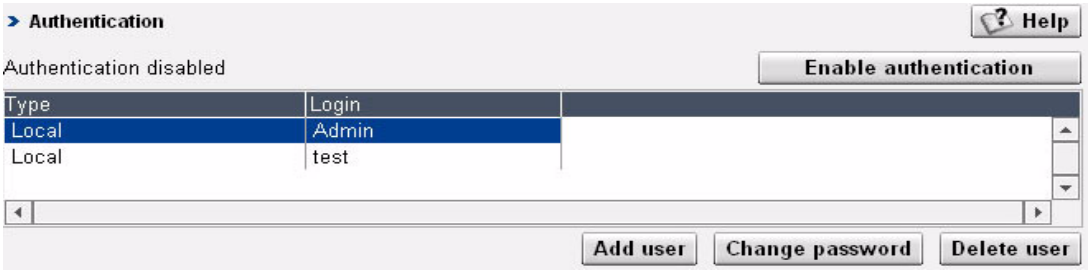
2. Enable the checkbox for **Enable SSL**.

3. Then, you can see the following message and SyncThru ™ Web Admin Service will reload the page automatically with an https connection.

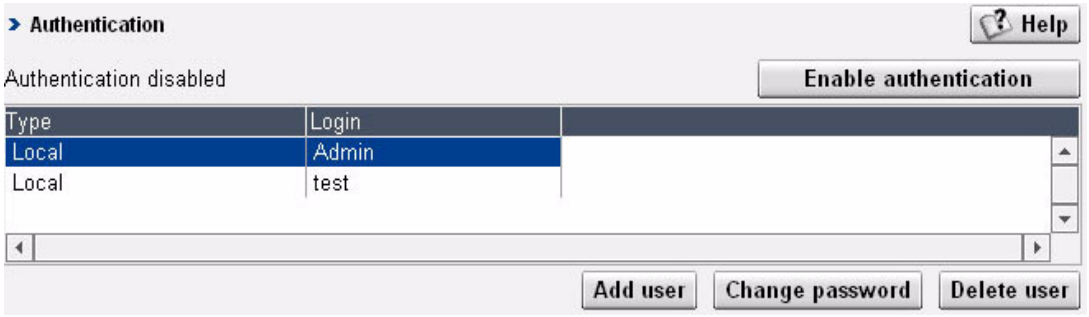


How to enable Authentication:

1. Go to the **Settings** > **Authentication** page.

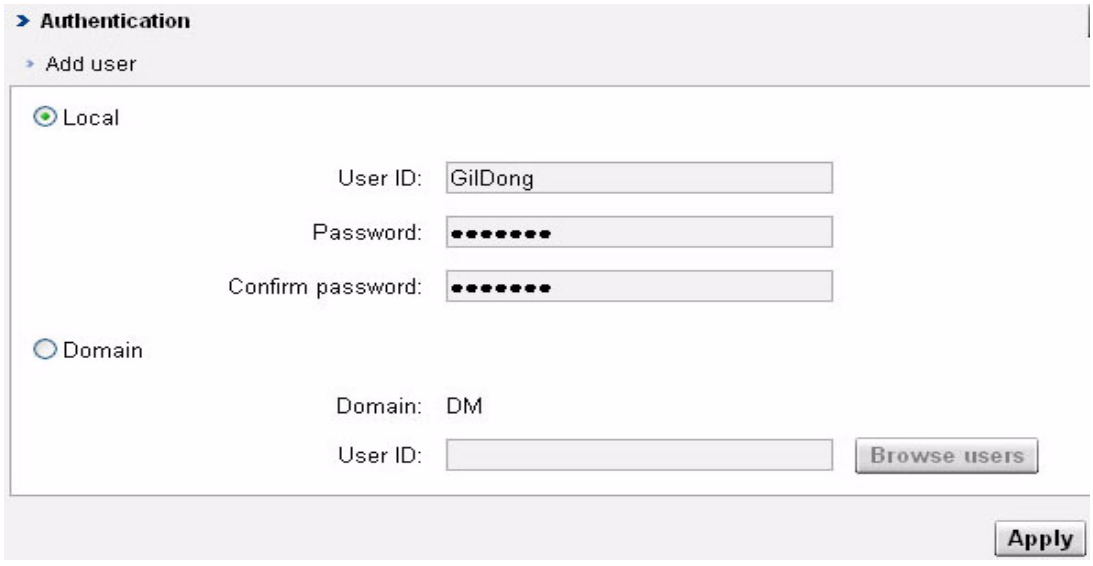


2. Now you can see the button of **Enable authentication** and you can enable by clicking that button.



3. SyncThru TM Web Admin Service will show the login page just after authentication is enabled.

4. You can also only see the **admin** as a default user in the authentication user list. Its default password is **admin**. If you want to create new users, you can do by clicking the **Add user** button.



What is the purpose of group management?

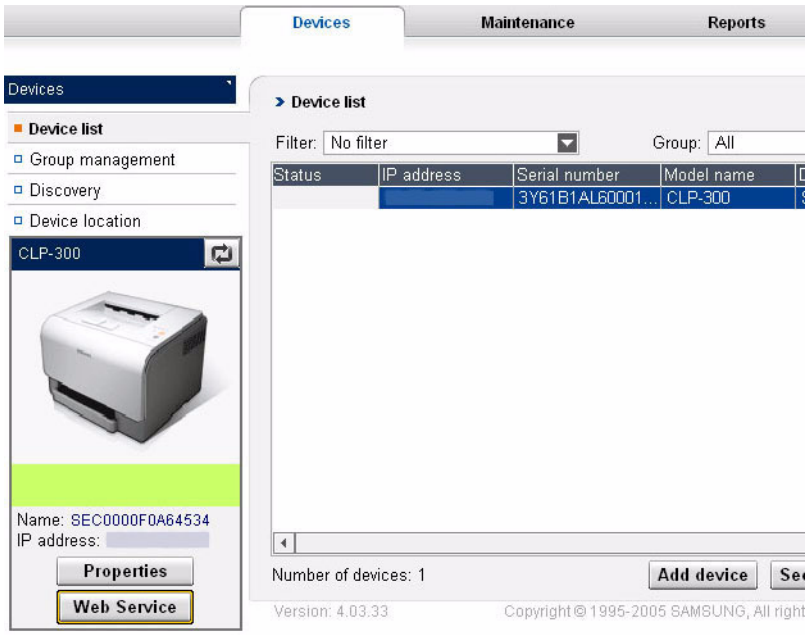
Device groups make it easier to find the devices, check their status, and perform maintenance and other administrative operations. For example, you can create groups around your own physical location and monitor/manage them easily.

> **Note**
> A single device can belong to an unlimited number of device groups.

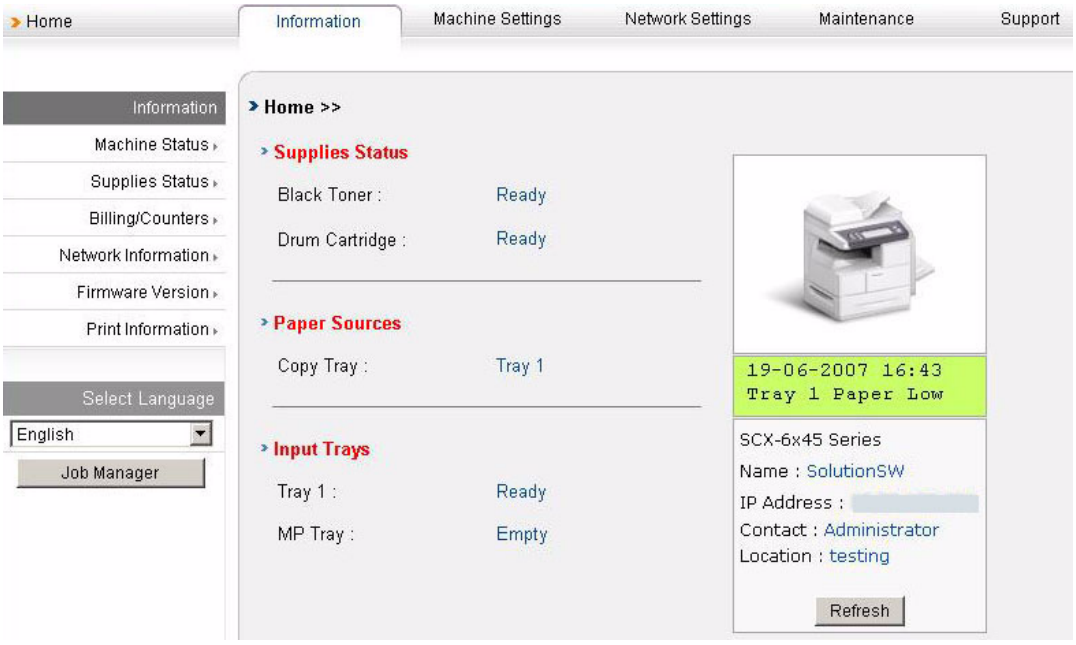
How do I manage jobs on the hard disk of each printer on SyncThru ™ Web Admin Service?

SyncThru ™ Web Admin Service provides the links to the embedded web server of devices. You can open the web service and use **Job Manager** as follows:

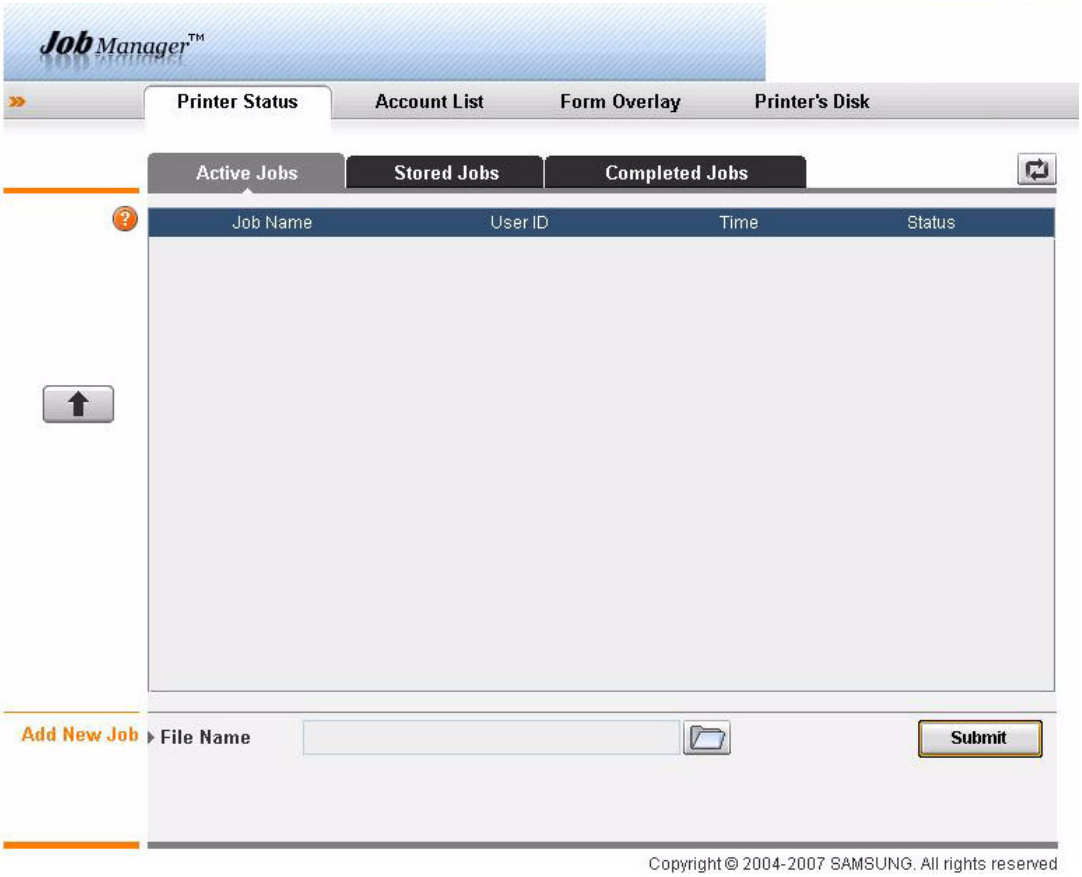
1. Go to the **Devices** > **Device list**.
2. Select a device with HDD. Job Managing depends on HDD installation. If a device has HDD installed, you can manage its jobs.
3. Click the **Web Service** button of the specified device in the left frame. Or open a new web browser and enter the device's IP address in the address bar. Then you can see the embedded web server, the web service of the device.



4. If it is a Samsung device with HDD, you can see the **Job Manager** button at left frame of the embedded web server page.



5. You can see the **Job Manager** page.



What is the SyncThru ™ Web Admin Service Plug-In and how does one use it?

The SyncThru ™ Web Admin Service Plug-Ins can be installed to provide additional functionality. Plug-ins can make SyncThru ™ Web Admin Service very extendable and flexible. For example, if you have no device with feature-supporting cloning, you do not have to install the Device Cloning Plug-In.

Current SyncThru ™ Web Admin Service Plug-Ins include:

- Device Cloning Plug-In
- Driver Management Plug-In
- File Storage Plug-In
- Job Accounting Plug-In
- Local Device Discovery Plug-In
- Report Generator Plug-In
- Device Location Plug-In
- SMS Plug-In

How to get these plug-ins

you can download plug-ins from the Samsung web site.

How to install plug-ins

SyncThru ™ Web Admin Service supports additional features by providing plug-in components. Each plug-in is provided as an executable file. To install and use each plug-in, refer to the manual for each plug-in.

Is it possible to add a list of multiple users?

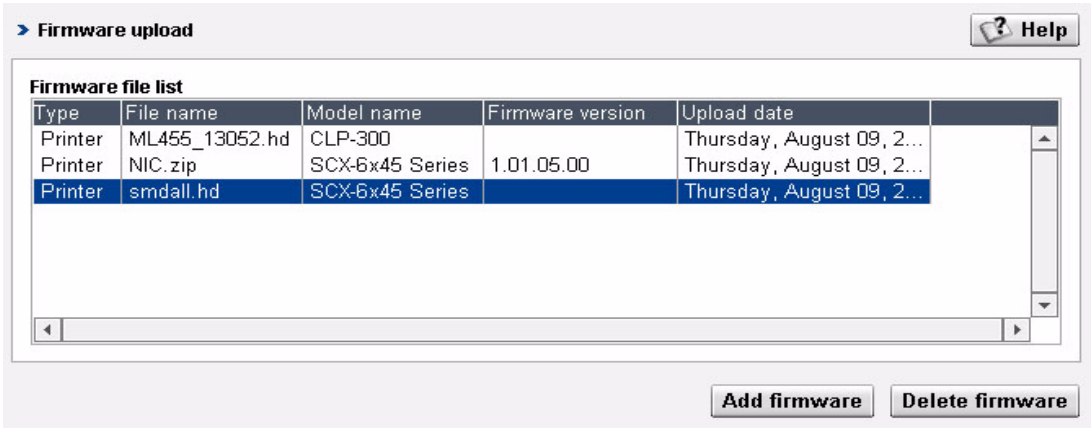
Unfortunately, SyncThru ™ Web Admin Service does not support importing multiple users. You need to add users one by one in **Settings > Authentication**.

How do I upgrade the firmware for devices?

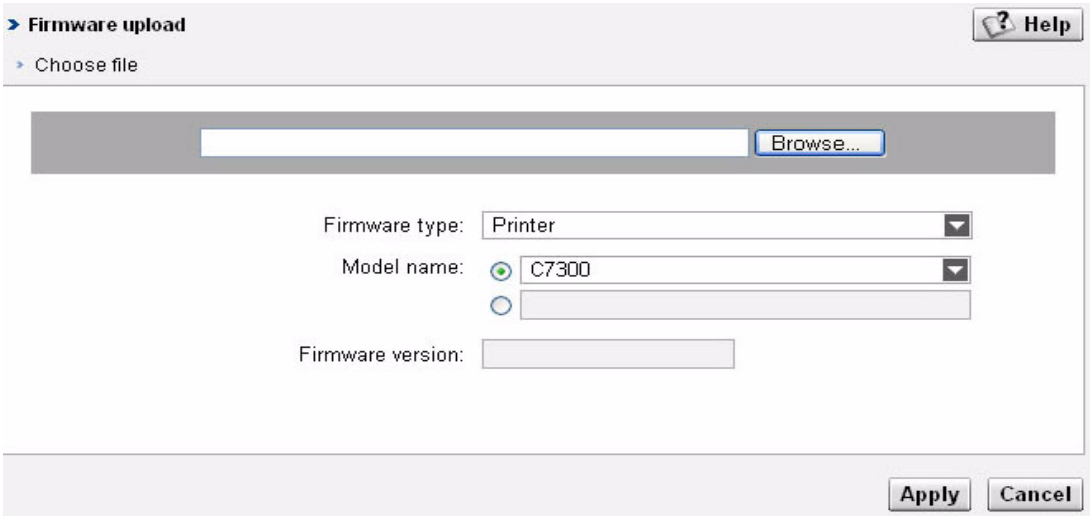
In order to upgrade new firmware for the specified devices, you need to get the firmware, which you want to download, from the sites of the device manufacturer or service center first. After that, you upload the firmware to the SyncThru Web Server. With this firmware, you can upgrade the devices which listed up in the **Device list**. For the detailed instructions, see the follows:

1. Get the firmware which you want to upgrade.
2. Go to the **Maintenance** > **Firmware upload**.

3. You can upload firmware by clicking the **Add firmware** button.



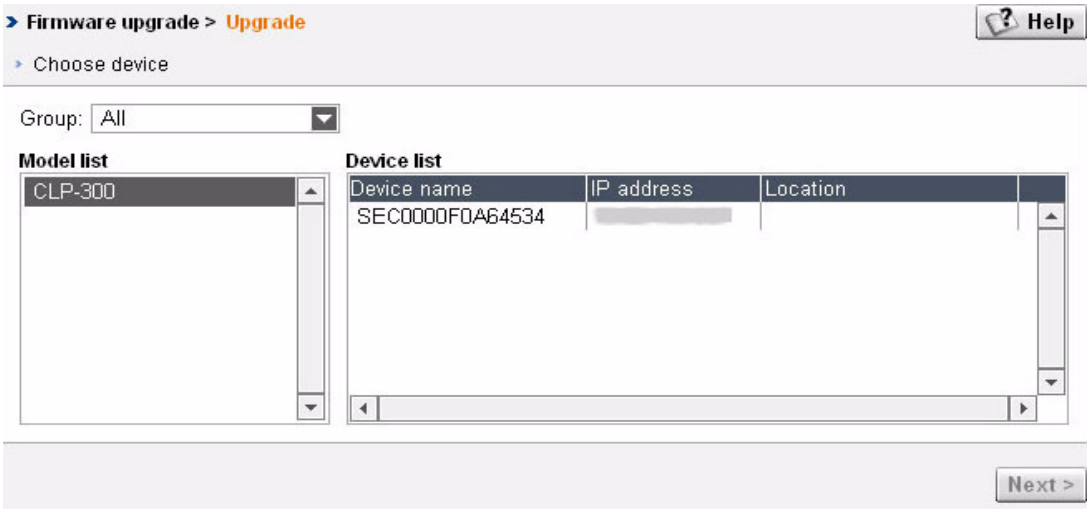
4. Click the **Browse** button and choose the firmware, and click the **Apply** button.



5. You can see the firmware list the SyncThru ™ Web Admin Service contains.

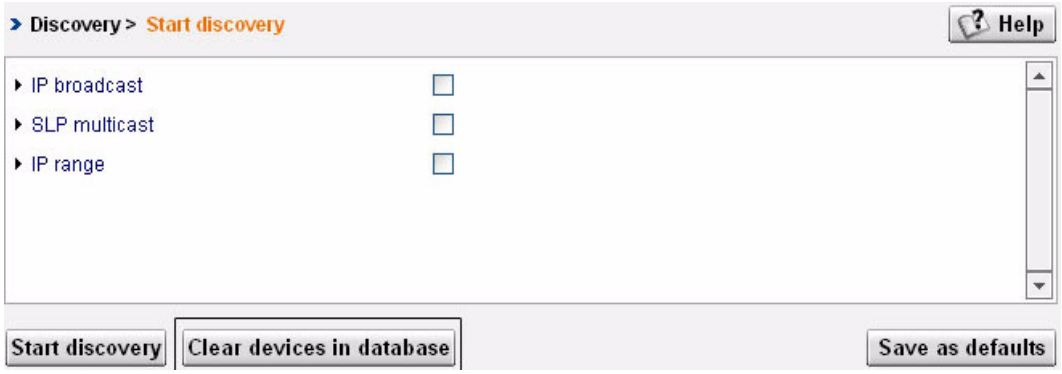
6. Go to the **Maintenance** > **Firmware upgrade** page.

7. Select the devices you want to upgrade and move on to the next steps.



What is the difference between Clear devices in database and Clear Database?

You can use it for deleting the devices previously discovered by SyncThru ™ Web Admin Service. SyncThru ™ Web Admin Service will eliminate the devices in its database. For example, if you want to delete all devices in the current SyncThru ™ Web Admin Service database and search a new device list, you can use this function. You can see **Clear devices in database** in the **Devices > Discovery > Start discovery**.



Another database function is cleaning database, which is located in the **Settings > Database management > Database cleaning**. If you want to remove all the data within the specific date, you need to configure these settings.

How do I contact the Samsung printer service for questions about SyncThru ™ Web Admin Service?

You can see the **Contact us** link on the top frame of the SyncThru ™ Web Admin Service. Then you can contact Samsung web site, http://www.samsungprinter.com and click **CONTACT US** again at the bottom frame.

How do I contact a representative of administrators or send him email?

To contact your SyncThru ™ Web Admin Service administrator, you can see your administrator information in the **Settings > Administrator information**. You can contact an administrator with the information.

Is Window XP Service Pack 2 supported with SyncThru ™ Web Admin Service?

SyncThru ™ Web Admin Service supports Windows XP Service Pack 2 if the firewall is disabled or if the following ports are enabled:

Port name	Description
8080	HTTP default port, or if you configure another port number for HTTP, the specified port number should be enabled.
8443	HTTPS default port, or if you configure another port number for HTTPS, the specified port number should be enabled.
427	SLP Multicast discovery port number.
161	SNMP IP broadcast discovery and agent listening port number.
162	Traps listening port number.

9 MIB References

Management Information Base(MIB) is a type of database used to manage the devices in a communications network. SyncThru [TM] Web Admin Service supports standard printers MIB-compliant.

This chapter includes:

- **Generic Support**
- **Supported Printers**

Generic Support

SyncThru uses SNMP queries to gather information from printers. How much information is displayed and what functionality is provided depend on the printer's own ability to respond to SNMP queries.

Supported Printers

Any printer directly connected to the network that supports SNMP and the standard printer MIB, RFC 1759, is supported.

- All Samsung Network Printers and MFPs
- Other SNMP compliant printers and MFPs

Network SNMP Printers and MFPs should support the following Request for Comments (RFC) standards:

- RFC 1213 (MIB-II for TCP/IP)
- RFC 1759 (Printer MIB v1)
- RFC 3805 (Printer MIB v2)
- RFC 3806 (Printer Finishing MIB)
- RFC 1514 / RFC 2790 (Host Resources MIB v1, v2)

10 Acronyms and Abbreviations

Terms Used	Description of terms
DBMS	DataBase Management System
HDD	Hard Disk Driver
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
MD5	Message Digest algorithm 5
RFC	Request For Comments
SHA	Security Hash Algorithm
SLP	Service Location Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
USB	Universal Serial Bus